

REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed June 2, 2005. In the Office Action, claims 1-21 were rejected under 35 U.S.C. §103(a). Applicant respectfully traverses the §103(a) rejection and respectfully requests the Examiner to withdraw the rejection.

Rejection Under 35 U.S.C. § 103

Claims 1-21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rallis (U.S. Patent No. 6,425,084) in view of Adams (U.S. Patent No. 6,363,485). Applicant respectfully traverses these rejections in their entirety because a *prima facie* case of obviousness has not been established. Claims 3, 5, 12, 15 and 19 have been amended and claims 22-23 have been cancelled.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine*, 873 F. 2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988). Herein, at a minimum, the combined teachings of the cited references do not describe or suggest all the claim limitations set forth in independent claim 1.

Herein, neither Rallis nor Adams, alone or in combination, suggests every limitation set forth in the above-identified claims. For instance, the Office Action states that column 3, lines 18-29 and column 5, lines 9-21 of Rallis teach an operation to “releasing a first keying material from a token communicatively coupled to the platform in response to authenticating the user”. Applicant respectfully disagrees with these findings because Rallis teaches the boot-up user-validation program where the first keying material is released *prior to* user authentication, not in response to authenticating the user. *Emphasis added*. According to the Office Action, the “key device serial number” is considered to be the first keying material (steps 2-3 of FIG. 3A) and the user

authentication is considered to be user validation after release of the first keying material (steps 5-6 of FIG. 3A). Hence, since neither Rallis nor Adams describe or suggest all of the claim limitations set forth in independent claim 1, a *prima facie* case of obviousness has not been established, and thus, the §103(a) rejection should be withdrawn.

Based on the dependency of claims 2-11 on independent claim 1, believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traverse is warranted. Applicant reserves the right to present such arguments in an Appeal is warranted. Withdrawal of the §103(a) rejection as applied to claims 1-11 is respectfully requested.

With respect to independent claims 15 and 19, Applicant incorporates the arguments set forth above in which the trusted platform module produces a combination key by combining a first incoming keying material *released after authentication of a user of the platform* with a second keying material. *Emphasis added.* In contrast and teaching away from the claimed invention, the teachings of Rallis are directed to the release of the first keying material (key device serial number) before any user authentication. Hence, withdraw of the outstanding §103(a) rejection as applied to independent claims 15 and 19 as well as claims 16-18 and 20-21 dependent thereon is respectfully requested.

With respect to independent claim 12, Applicant respectfully submits that neither Rallis nor Adams, alone or in combination, disclose or suggest a *trusted platform module* that is communicatively coupled to the boot block memory unit and that *includes* (i) an *interface* adapted to provide a communication path to the boot block memory unit, (ii) a *processor* and (iii) an *internal memory*. *Emphasis added.* The trusted platform module is further adapted to produce a combination key *internally within the trusted platform* module by combining a first incoming keying material with a second keying material internally stored within the integrated circuit and to decrypt a second BIOS area using the combination key to recover a second segment of BIOS code. *Emphasis added.*

In contrast, the teachings of Rallis are directed to the input of the first keying material (key device serial number) before any user authentication. But such input has not been considered for insertion into an integrated circuit that is further used to Applicant has been able

Appl. No. 09/751,899
Amdt. Dated 09/02/2005
Reply to Office Action of 06/02/2005

to locate any teachings within Rallis or Adams of producing the combination key internally within the trusted platform module as claimed. Hence, withdraw of the outstanding §103(a) rejection as applied to independent claim 12 as well as claims 13-14 dependent thereon is respectfully requested.

Conclusion

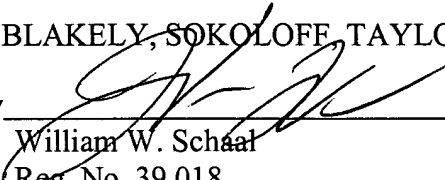
Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 9/2/05

By


William W. Schaal

Reg. No. 39,018

Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

FACSIMILE

☒ deposited with the United States Postal Service
as first class mail in an envelope addressed to:
Commissioner for Patents, PO Box 1450,
Alexandria, VA 22313-1450.

☐ transmitted by facsimile to the Patent and
Trademark Office.

Date: 9/2/2005


Susan McFarlane

9/2/2005

Date